SANDIA REPORT

SAND97-0714 • UC-700
Unlimited Release
Printed March 1997

Production Risk Evaluation Program (PREP) Summary

Edwin A. Kjeldgaard, Jose H. Saloio, Michael G. Vannoni

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A04
Microfiche copy: A01

SAND97-0714
Unlimited Release
Printed March 1997

Distribution
Category UC-700

Production Risk Evaluation Program (PREP)

SUMMARY

Edwin A. Kjeldgaard
Transportation Systems Analysis Department

Jose H. Saloio
Nuclear Safety and Systems Safety Analysis Department

Michael G. Vannoni
Nonproliferation and Arms Control Analysis Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0718

ABSTRACT

Nuclear weapons have been produced in the US since the early 1950s by a network of contractor-operated Department of Energy (DOE) facilities collectively known as the Nuclear Weapon Complex (NWC). Recognizing that the failure of an essential process might stop weapon production for a substantial period of time, the DOE Albuquerque Operations office initiated the Production Risk Evaluation Program (PREP) at Sandia National Laboratories (SNL) to assess quantitatively the potential for serious disruptions in the NWC weapon production process. PREP was conducted from 1984-89. This document is an unclassified summary of the effort.

INTRODUCTION AND OBJECTIVE

Nuclear weapons have been produced in the US since the early 1950s by a network of contractor-operated Department of Energy (DOE) facilities collectively known as the Nuclear Weapon Complex (NWC). Recognizing that the failure of an essential process might stop weapon production for a substantial period of time, the DOE Albuquerque Operations office initiated the Production Risk Evaluation Program (PREP) at Sandia National Laboratories (SNL) to assess quantitatively the potential for serious disruptions in the NWC weapon production process. PREP was conducted from 1984-89. This document is an unclassified summary of the effort. At the time of the study, the NWC consisted of nine facilities: Rocky Flats Plant in Golden, CO; Pantex Plant in Amarillo, TX; Savannah River Plant in Aiken, SC; Pinellas Plant in Largo, FL; Mound Facility in Miamisburg, OH; Kansas City Plant in Kansas City, MO; Oak Ridge Y-12 Plant in Oak Ridge, TN; Oxnard Facility in Oxnard, CA; and Bendix Albuquerque Operations in Albuquerque, NM.

The goals of PREP were defined as:

(1) Identify credible vulnerabilities in production activities (collectively called "critical links"). Vulnerabilities are production equipment, support systems, and facility buildings whose failure or loss would prevent the nuclear weapon production necessary to maintain national security.

(2) Develop a methodology for performing quantitative risk assessment of weapon manufacturing operations in the NWC as an integrated system.

(3) Develop new analytical tools for implementing efficient risk reduction strategies within the NWC.

(4) Achieve sufficient flexibility and ease of use in the risk assessment process to enable the DOE facilities to perform such analysis in the future.

The maintenance of a viable nuclear deterrent force, in support of national policy, is DOE's primary production goal. No disruption should cause production to be behind schedule for more than a specified time period. The PREP project analyzed the NWC for potential vulnerabilities in weapon production. Production risk results from the failure of elements of the manufacturing system: production equipment, support systems, raw material and component inventories, suppliers, or facility buildings. The failure or unavailability of a key element could prevent the production of sufficient nuclear weapons to maintain a credible deterrent and preserve national security. (Failure was defined as being behind schedule in specified products for a specified period of time.)

This summary describes the methodology PREP developed to perform production risk assessment. It also discusses the techniques developed by PREP to support the establishment of a risk reduction strategy in manufacturing systems. While the PREP analysis tools were developed for application in the NWC, the techniques are generic and are not limited to weapon production. A section of this report describes application of the models to the allocation of resources, security planning for industrial sabotage protection, risk assessment in nuclear material production or reprocessing, and commercial manufacturing.

PREP RISK ASSESSMENT METHODS

The task of identifying critical links required that PREP create new analytical techniques to assess the risk associated with a manufacturing system. PREP developed an analytical procedure incorporating network and fault tree models to identify the dominant sources of production risk and offer remedial strategies to

reduce that risk in the most effective way. Computer programs were written to represent each of the models, and the necessary data bases were created. Application of the PREP risk assessment tools requires that the analyst follow a set of specified procedures and provide data describing various production characteristics. Extensive risk assessment experience is not necessary, and the required calculations are performed using a personal computer.

The risk associated with an undesired event is expressed as the product of its probability of occurrence and the consequence given it does occur. The PREP analysis is not a risk assessment in the classical sense where system risk is measured as the summation of risk contributed by all conceivable failure events. The purpose of the program was to develop and apply a systematic set of analytical methods to identify the most likely potential contributors to long-term disruption of essential weapon production. The limiting ground rules and assumptions used in PREP were intended to focus the analysis on the events that have both significant consequences and significant probabilities of occurrence. For example, failure events assessed to have very low probabilities of occurrence were not classified as critical links. Because of the analysis guidelines and the uncertainty in assessing infrequent events, the quantitative results of the PREP analysis should not be viewed as predictive of NWC performance or as absolute measures of production risk; the PREP results are relative indices that point toward the critical links in the NWC.

Disruptions of short duration that do not affect the production system's overall output occur routinely in all manufacturing operations. The PREP analysis procedures screen out minor disruptions and focus on long-term, credible failures that would cause the production system to stop for an extended period. Three key attributes of a production critical link are analyzed: probability of failure, the failure's effect on production, and duration of outage.

Highly improbable failures are not considered credible. The NWC analysis used a probability value of 1 in 100,000 per year as the threshold for credible failure occurrences. This threshold probability value, selected in consultation with DOE, served as one criterion for measuring acceptable system performance. Although somewhat arbitrary, it permitted potential failures to be divided into significance categories. This approach has been used by others. For example, the annual probability of an employee fatality in all industries per year in the United States is 1 in 100,000. The International Council For Radiation Protection (ICRP) used this probability guideline in developing radiation health protection standards for workers in the nuclear industry. The rationale for this choice was that the risk to nuclear workers should be no higher than for workers in general.

The duration of the outage time resulting from the failure of an individual production process is one factor (along with production capacity, yield, inventory level, and production operation time) in determining whether the system of facilities in the NWC can catch up and meet its obligations within a specific time period. The DOE guidelines for the PREP analysis stated that the NWC system had a specified time to catch up with the scheduled number of weapons and limited-life components (LLCs) to be produced. Failures that caused the NWC system to be behind schedule for less than that time were not considered to be critical links.

The two-stage PREP analysis first addresses the duration of outages, then the probability and production consequence of failure events. Figure S-1 illustrates the approach used in the production system disruption analysis.

Network Flow Analysis of Production

Manufacturing is performed by moving a product through a sequence of operations (e.g., pressing explosive materials, machining metal parts, testing, etc.). In the first stage of the NWC analysis, we studied the operations used to

manufacture the defined package of weapons and LLCs. This information was used to construct a network model that represents the flow of parts through the NWC from input materials to completed weapons. The PREP network model is composed of production operations called "arcs." As shown in Figure S2, arcs are composed of one or more "activities" which correspond to a group of similar equipment performing the same function. The network model assumes steady-state behavior and computes the "critical time" for each arc in the production system. The critical time is the longest period of time an arc and any of its constituent activities can stop without preventing the NWC system from achieving its production goals. An outage longer than this period of time would thus cause the NWC to fail to meet its obligations as defined by DOE for the PREP analysis.

The production of an assembly at a plant serves as an example of network structure. One operation is to make a formed part from a metal sheet. The arc in the network is called "part XYZ fabrication" and consists of three activities: (1) outside contour machining [3 lathes], (2) inside contour machining [4 lathes], and (3) drilling [1 drill]. We then collected data from the plant (and the other plants for their operations) to characterize and quantify each of its arcs in the NWC network. These data consist of the scheduled production for the arc, ratio (the number of an arc's products required to produce a single output unit in the next arc), yield, "sprint" capacity (the maximum productive capacity), normal and minimum process times, and average inventory of inputs.

Fault Tree Analysis of Production Arcs

In the second stage of the analysis, fault tree modeling is used to identify events that could cause an activity to stop for longer than its critical time. A fault tree model provides a general means of stating and analyzing the production reliability problem in a comprehensive manner which is applicable to any type of facility. The fault tree model identifies the credible set of production equipment, for any type of failure, which causes an activity to become a critical link.

A fault tree is a logic diagram which graphically represents the combinations of events that can result in a specified failure of the system. During fault tree analysis, this specified system failure is successively decomposed into combinations of contributing failure events until basic events (e.g., individual machine failures) terminate each branch of the tree. Each branch of the tree is developed by identifying the immediate, necessary, and sufficient conditions leading to each failure event. Logical operators (e.g., AND or OR) combine events to produce a resultant state. The fault tree thus provides a means of cataloging a large number of failure scenarios in a structured manner.

The fault tree analysis examines the effect on the production system of both independent failure events (the random failure of a single item of equipment, failure of required tooling or fixtures, operator error, test/maintenance outage) and the special situation of common cause failure events. Common cause failures affect an entire set of equipment. The set may be defined by a physical production zone at a facility or a geographically separated group of equipment associated by the same support system. The effects of industrial accidents (e.g., fire or chemical spill), natural phenomena, and support system-induced damage to production equipment (e.g., a voltage surge in the electrical system) are examined under the common cause category. In order to assess the effect of a zone's disablement, the production system's failure modes must first be known. Therefore, the common cause failure phase of the fault tree analysis requires that the fault tree model be complete, and it is performed subsequent to the independent failure analysis.

The probability of basic failure events is a major factor in the fault tree analysis. The PREP procedures to build the fault tree model adjust the level of analysis according to a threshold value for probability significance specified by

the analyst. If the estimated probability of a basic event (or a combination of basic events) resulting in an unacceptable production outage is greater than this threshold value, fault tree modeling of the event is continued to determine if the activity is a critical link. Otherwise additional fault tree modeling of that branch is terminated.

The fault tree modeling procedures account for probable emergency plant responses to production failures. Recognizing that plants can often work around a production failure, fault tree modeling for situations from which a plant can recover within the critical time of the production arc(s) affected by the failure is not continued. The procedures incorporate a series of screening questions to guide construction of the fault tree. The impact of political or regulatory constraints on plant recovery actions may be significant but is not considered by the screening questions. For example, regulations governing the handling of waste products may prevent some alternate equipment and facilities from being used.

User experience and the requirement for detailed information are limitations on the use of conventional fault tree analysis to study the potential for production disruptions. In addition to understanding all details of the plant production systems, the analyst must be familiar with fault tree analysis techniques. The detailed analysis of a large facility is a time-consuming process that requires several man-months. Furthermore, the results may depend on the experience level of the analyst who performed the work. To mitigate these limitations, PREP uses a technique known as modular logic to speed the fault tree modeling process and ensure consistency.

All production facilities have a number of features in common (e.g., basic machine tools, power inputs, material conveyance, and environmental controls). Because of these common characteristics, fault trees for different production facilities have very similar structure. The modular logic approach captures the characteristics common to production failures in a framework that can be adjusted to represent the specific conditions that exist in an individual production arc. Predefined modules representing the common types of failure logic in the system are assembled to produce a fault tree for a specific arc's failure modes, following the hierarchy shown in Figure S-3. An arc is decomposed into its constituent activities, then into equipment items and support systems. The result of this process is a fault tree model ready for direct analysis or input to a computer program (several programs exist) using Boolean algebra to identify the failure modes and their associated probabilities.

General procedures have been developed to aid the analyst in gathering the appropriate plant-specific information and formatting the generic fault tree modules to produce a detailed production vulnerability model of a particular plant. The modular logic technique is generic and overcomes the limitations of conventional fault tree analysis. In particular, it (1) permits someone with little knowledge of fault tree analysis to efficiently develop the detailed trees, (2) reduces the time required to develop specific trees, and (3) makes it unlikely that a production failure event is overlooked in the development of the production fault trees for specific plants.

Analysis of Failures Caused by Natural Phenomena

Part of the fault tree analysis deals with natural phenomena (high winds, tornadoes, earthquakes, and floods) which can disrupt production. In-depth analysis of a structural failure of a facility site or pertinent building (one that houses production processes associated with the products specified in the PREP package) from such events was beyond the scope of PREP. The PREP natural phenomena investigation was based on existing information: plant safety analysis reports, hazard analyses, and building design records. The assessment is a simple, highly conservative approach designed to identify potential vulnerabilities for which more detailed site analysis would be beneficial to the

plant. It is analytically unsound to draw more detailed conclusions because of differences in the way existing natural phenomena analyses were performed.

The PREP natural phenomena assessment involved several steps. First, the point of total destruction (wind speed, earthquake magnitude, or flood level) for pertinent buildings subjected to each type **of** natural phenomenon was estimated. Then the likelihood of a natural phenomenon of that magnitude occurring at a particular plant site was estimated. We conservatively assumed that all equipment within a building subjected to a natural phenomenon of that magnitude would be destroyed. Results from the independent failure assessment was used to identify affected equipment within the building which could not be replaced within the appropriate critical time. If the likelihood of the event exceeded the PREP probability threshold, and unaffected alternate equipment was not available, we classified the building and its production activities as critical.

Measurement of Production Risk

The concept of "system time behind schedule" permits us to rank critical links in terms of their contribution to production risk. System time behind schedule is the length of time a manufacturing system would be behind its scheduled production quantities if a critical link were to fail. We developed a method and computer program to compute the system time behind schedule for each critical link failure and rank the consequences of the failure relative to other such failures. This risk measure may be used as a surrogate value for the national security consequences of a NWC production outage.

PREP also developed two additional computer programs that serve as tools for formulating risk-reduction strategies relative to budget constraints. Reducing the risk associated with specific critical links can be accomplished by a variety of remedial actions: increasing sprint capacity, developing strategic inventories, and adding redundancy.

Although risk can be reduced, it can never be eliminated. Residual risk refers to the sources of production risk that would remain if all of the identified critical links and critical common cause failure mechanisms were removed from the NWC manufacturing system. Residual risk in an analysis thus arises from two basic sources: (1) failures whose potential is acknowledged but, for various reasons, not modeled, and (2) failures which are not quantifiable. We identified the sources of residual risk inherent in the PREP model and data. The conservatism in the PREP analysis process prevented the estimated residual risk from being great enough to challenge the overall credibility of the results.

RISK REDUCTION OPTIONS BASED ON PREP ANALYTICAL TOOLS

The issues associated with the identification of critical links (e.g., assessing capacity, chokepoints, level of inventory, yield, and process flowtimes) are basic parameters in production management and planning. Consequently, many aspects of the PREP methodology have general application in the management process. The physical configuration of the NWC production system, management practices such as inventory policy, and the condition of plant and equipment, are all factors in the system's vulnerabilities. Such vulnerabilities result in additional operating costs in the form of unexpected repairs and lost production. Prudent management should therefore address, in the strategic planning process, the cost-benefit issues associated with risk reduction.

GENERAL APPLICATION OF PREP METHODS TO OTHER STRATEGIC PLANNING ISSUES RELATED TO WEAPONS PRODUCTION

The PREP analytical methods offer a basis for a quantitative approach to other aspects of

strategic planning. Potential uses of the PREP methods in risk assessment and risk management include allocation of resources, risk assessment of nuclear material production, protection from sabotage, and prioritization of environmental issues relating to production.

Allocation of Resources

The PREP models were developed to provide a systematic, quantitative framework for allocating a fixed budget across a set of alternative improvement projects. With relatively little additional development, PREP analytical tools can also be used in the capital budgeting and facility restoration processes. Basic risk reduction options include increasing the sprint production capacity of the system, establishing redundant capability, and establishing protective inventories. Redundant capability can sometimes be acquired at low marginal cost if incorporated into normal procurement. The ability of a new machine to act as a backup is additional justification for its acquisition.

Risk Assessment of Nuclear Material or Other Production

PREP modeling procedures can be applied to other types of production. As part of the project, some developmental work on network and fault tree models that represent continuous material flow as well as discrete parts flow was performed. With these models, production risk assessment could be performed on nuclear material production for defense purposes or on chemical production for the commercial sector.

Protection From Sabotage

If sabotage is judged to be a significant threat, DOE or the NWC contractor facilities can use the PREP analysis to identify potential targets and measure the consequences of their loss. The analysis also indicates ways that consequence mitigation can be incorporated in a security strategy. Traditional security measures have focused on the prevention of an act of industrial sabotage. It is difficult to quantify the effectiveness of such protective measures, especially against the threat of sabotage by an employee with facility access. Consequence mitigation uses the reverse approach: the system is designed to accept a sabotage-induced failure and still fulfill its function. In this approach to security protection, damage to production equipment is offset by redundant resources (e.g., replacement equipment stored in a separate, protected area) that permit the facility to continue production without unacceptable interruption. A benefit of this approach is that protection against both sabotage and routine production failures can be enhanced without interfering with normal production operations.

Prioritization of Environmental Issues Relating to Production

The DOE facilities face more intense oversight and operational constraints by environmental regulatory agencies than in the past. Compliance with regulatory standards requires the investment of facility resources in waste processing. A potential failure mode for production which PREP identified is the inability of a waste processing support system to process, emit, store, or transport hazardous or radioactive waste byproducts. Production is thus stopped by indirect means because of waste backup or by regulatory decree. Although employee and public safety are the prime consideration in environmental issues, the potential impact on production operations should be a major factor in the prioritization of remedial actions. Proposed regulatory policy might be amended when actions that would adversely affect national security are identified by means of the PREP analysis tools.

CONCLUSION AND RECOMMENDATIONS

PREP identified the dominant sources of production risk in the NWC and provided the analytical tools to update the risk assessment in the future. The results provide a framework for selecting remedial strategies to reduce risk,

thereby making the NWC production system more tolerant of process failures. DOE, in concert with the design laboratories and the NWC plants, can also begin a risk reduction program based on the PREP methodology. An ongoing risk reduction program would help maintain our national security by ensuring the continued maintenance of the stockpile and production of new nuclear weapons.

Such a risk reduction program would require the production process models to be updated periodically to reflect changes in technology and the physical plant. Furthermore, production risk analysis should be oriented toward the examination of the impact of projected changes (e.g., the effect on production reliability of implementing computer-controlled production lines). The PREP analysis used a manual system of data collection which required a relatively high level of plant manpower support. An electronic data acquisition system should be developed to access production data that already exist (or will soon exist) in an electronic format in plant production control systems.

POSTSCRIPT

Shortly after PREP concluded, the DOE stopped producing weapons. Thus many of the recommendations were irrelevant in the context of the production system. Key elements of the PREP technology, however, evolved into a method for analyzing the vulnerability of the nuclear weapon dismantlement process, which in turn evolved into the Pantex Process Model (PPM).[1,2] The PPM is a computerized manufacturing optimization model which supports planning and scheduling of all production activities at Pantex, including nuclear weapon dismantlement and stockpile surety programs.

REFERENCES

1. E. A. Kjeldgaard, G. F. List, M. A. Turnquist, and D. A. Jones. *Planning Tools and Techniques for Product Evaluation and Disassembly*, SAND96-1343C, Nov. 1996, Sandia National Labs (Presented at INFORMS Atlanta, Fall 1996.)

2. E. A. Kjeldgaard, G. F. List, M. A. Turnquist, and D. A. Jones. *Planning Tools and Techniques for Agile Manufacturing*, SAND96-2032C, Oct. 1996, Sandia National Labs (Presented at the Conference on Agile and Intelligent Manufacturing Systems, 10/2-3/96, Troy, NY.)

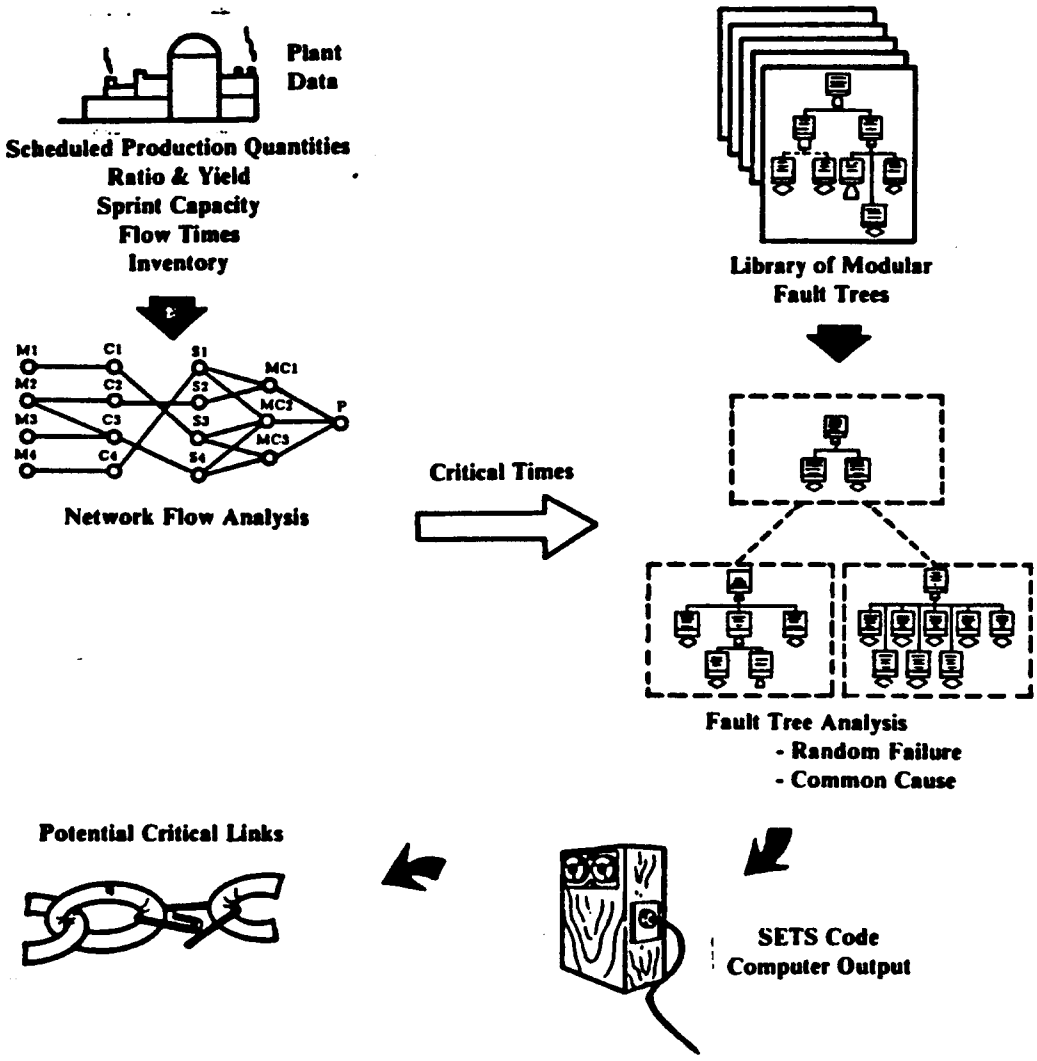

Figure S-1. Flow of PREP Analysis

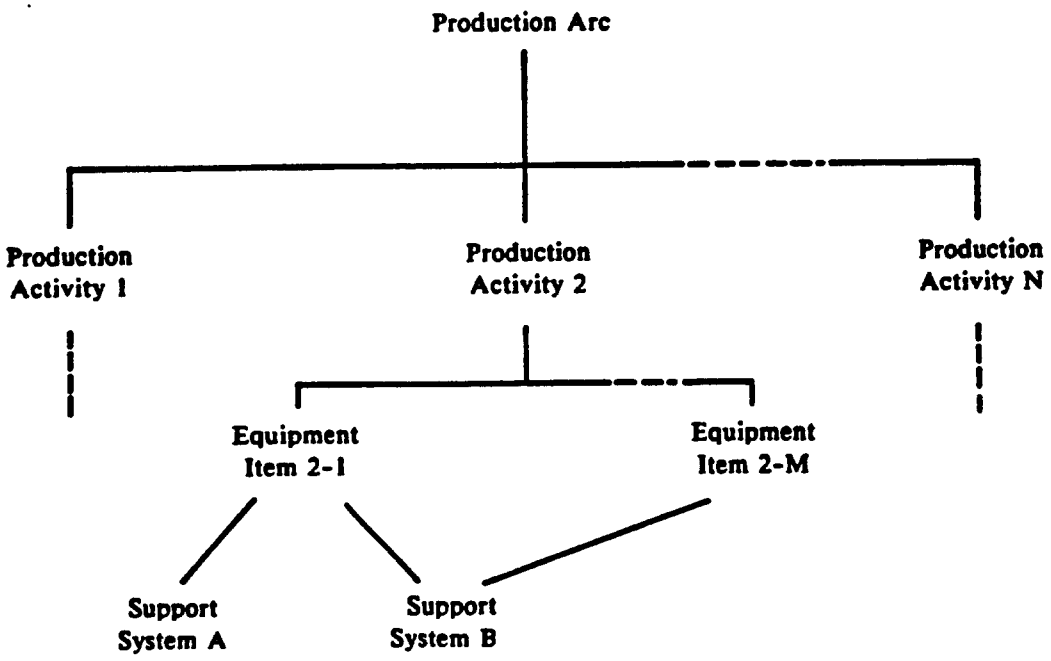

Figure S-2. General Structure of Network Production Arc

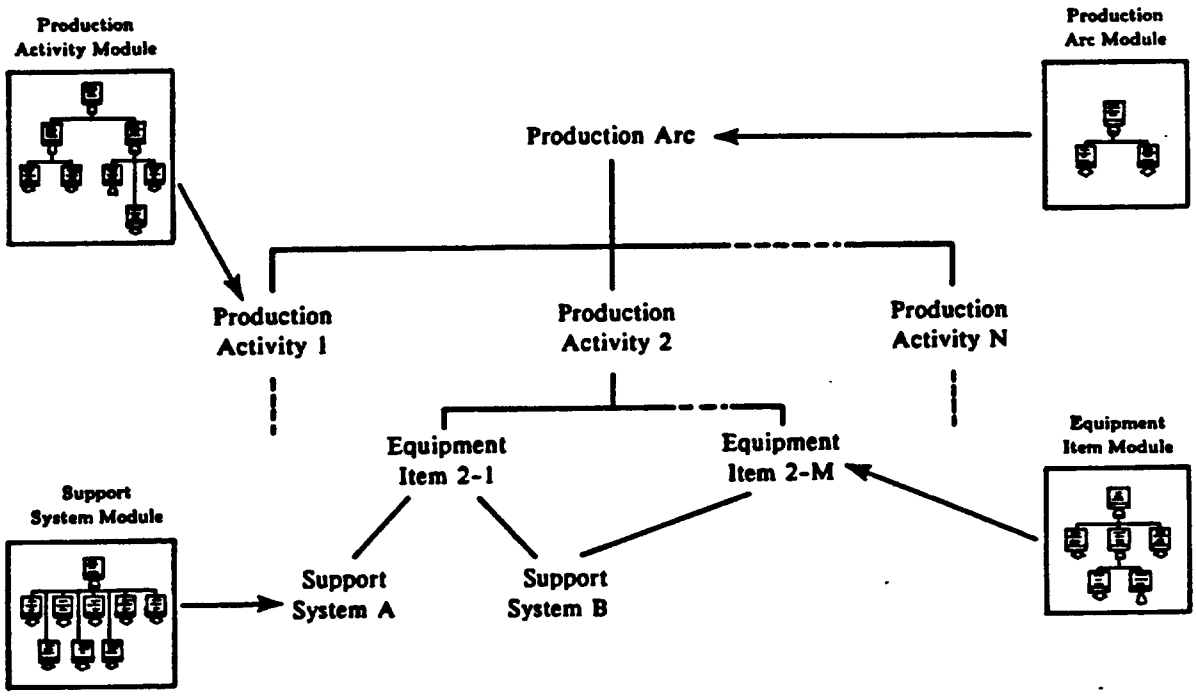

Figure S-3. Generic Modules Used to Construct Detailed Fault Trees

Distribution:

Housekeeping

1	MS 9018	Central Technical Files, 8940-2
5	MS 0899	Technical Library, 4414
2	MS 0619	Review and Approval Desk, 12690 For DOE/OSTI

Internal:

1	MS 0715	Bob Luna
1	MS 0718	Richard Yoshimura
5	MS 1373	Mike Vannoni
5	MS 1146	Joe Saloio
25	MS0718	Ed Kjeldgaard